CLAIMS

1. Method for switching a computer system (11; 21; 60), which is connectable via a communication interface (64) and a network (12; 22; 62) to a server module (13; 23; 61), into a special mode of operation, the method comprising the steps:

a. exhausting step-by-step a credit of a credit counter (44) of the computer system (11; 21; 60) ;

b. switching the computer system (11; 21; 60) into the special mode of operation if the credit is exhausted;

c. sending an identifier (w) assigned to the computer system (11; 21; 60) via the communication interface (64) and the network (12; 22; 62) to the server module (13; 23; 61);

d. receiving a token (S) issued by the server module (13; 23; 61);

e. verifying the validity of the token (S); and

f. if the token (S) is valid, then extracting a credit (C) from the token (S) and updating the credit counter (44) with the credit (C).

2. The method of claim 1, whereby the computer system (11; 21; 60) is caused to switch into the special mode of operation if step e. reveals that the token (S) is invalid.

3. The method of claim 1, whereby the computer system (11; 21; 60) continues with step c. if step e. reveals that the token (S) is invalid.

4. The method of claim 1, whereby step c. is carried out before the credit counter (44) reaches a predefined value or threshold (v).

5. The method of claim 4, whereby the predefined value or threshold is zero (v=0).

6. The method of claim 1, whereby the validity of said token (S) is verified by checking whether the token (S) comprises a signature of the server module (13; 23; 61).

7. The method of claim 1, whereby the credit counter (44) is updated by adding the credit (C).

8. The method of claim 1, whereby the credit counter (44) is updated by overwriting it with the credit (C).

9. The method of claim 1, whereby the identifier (w) is unique within the network (12; 22; 62).

10. The method of claim 2, whereby the special mode of operation is a mode of operation where:

- the computer system (11; 21; 60) or part(s) thereof are inactivated; or
- certain services provided by the computer system (11; 21; 60) are canceled; or
- the computer system's (11; 21; 60) access to sensitive services is refused; or
- the computer system (11; 21; 60) shows an alert screen or issues an alarm; or
- the computer system (11; 21; 60) causes an alert message to be sent out; or
- software of the computer system (11; 21; 60), or part of the software, is rendered useless.

11. The method of claim 1, whereby the computer system (11; 21; 60) is switched into the special mode of operation if the computer system (11; 21; 60) was reported lost or stolen.

12. The method of claim 1, whereby step c. comprises the steps:

- generating additional information (n);

- encrypting the identifier (w) and the additional information (n) to generate a secure identifier (E) using a cryptographic key (k).

13. The method of claim 12, whereby the cryptographic key (k) is a secret cryptographic key, preferably a cryptographic key of a public encryption scheme.

14. The method of claim 12, whereby the additional information (n) is a random number, preferably an unpredictable random number.

15. Method in a system (13; 23; 61) that is connectable via a network interface (67) and a network (12; 22; 62, 66, 68) to a computer system (11; 21; 60), the method comprising the steps:

- receiving an identifier (w) from the computer system (11; 21; 60) via the network (12; 22; 62, 66, 68) and the network interface (67);

- comparing the identifier (w) with a list (14; 24) of identifiers (w) to determine whether the identifier (w) originates from a computer system (11; 21; 60) that was reported lost or stolen;

  - if the identifier (w) originates from a computer system (11; 21; 60) that was not reported lost or stolen, then generating a token (S) which comprises the identifier (w) and a credit C, signing the token (S) using a cryptographic key to create a signed token (S), and sending the signed token (S) via the network interface (67) and the network (12; 22; 62, 66, 68) to the computer system (11; 21; 60).

16. The method of claim 15, whereby the following step is carried out if the identifier (w) originates from a computer system (11; 21; 60) that was reported lost or stolen:

  - generating a token (S) which comprises the identifier (w) and a credit revocation, signing the token (S) using the cryptographic key to create a signed token (S), and sending the signed token (S) via the network interface

(67) and the network (12; 22; 62, 66, 68) to the computer system (11; 21; 60).

17. The method of claim 16, whereby the credit revocation is a negative credit amount.

18. The method of claim 16, whereby the system is a server or server module.

19. The method of claim 15, whereby the cryptographic key is a public key.

20. The method of claim 16, whereby the list (14; 24) of identifiers (w) is a black-list which comprises the identifier (w) of a plurality of computer systems that are reported lost or stolen.

21. The method of claim 16, whereby the list (14; 24) of identifiers (w) is a valid list which comprises the identifier (w) of a plurality of computer systems that are not reported lost or stolen.

22. The method of claim 16, whereby the system applies predefined rules when generating a token (S) which comprises the identifier (w) and a credit C.

23. The method of claim 16, whereby the signed token (S) comprises additional information (n) that was received from the computer system (11; 21; 60) together with the identifier (w).

24. The method of claim 23, whereby the step of generating a token (S) comprises the steps:

- generating the binary XOR (H) of the identifier (w) and the additional information (n).

25. The method of claim 24, whereby the step of generating a token (S) comprises the steps:

- concatenating the binary XOR (H) and the credit (C) to generate the concatenation (H||C); and

- creating the signed token (S) by signing the concatenation (HllC) using the cryptographic key.

26. Apparatus comprising:

- a communication interface (64) for connecting the apparatus (11; 21; 60) via a network (12; 22; 62) to a server module (13; 23; 61),

- a software component (26; 50) for sending an identifier (w) assigned to the apparatus (11; 21; 60) via the communication interface (64) and the network (12; 22; 62) to the server module (13; 23; 61), and for receiving a token (S), issued by the server module (13; 23; 61), whereby the token (S) comprises a credit (C);

- a trusted hardware component (25; 40) storing the identifier (w) and comprising a credit counter (44) with a credit

  - which is automatically exhaustible step-by-step by the apparatus (11; 21; 60); and

  - which is updateable with the credit (C);

- a trigger unit (25; 47) for switching the apparatus (11; 21; 60) into a special mode of operation if the credit of the credit counter (44) is exhausted.

27. The apparatus of claim 26, wherein the communication interface (64) comprises a transmitter and a receiver.

28. The apparatus of claim 26, wherein the trusted hardware component (25; 40) also stores a cryptographic key (k).

29. The apparatus of claim 28, wherein the software component (26; 50) encrypts the identifier (w) using the cryptographic key (k) prior to sending the identifier (w).

30. The apparatus of claim 26, wherein the trusted hardware component (25; 40) further comprises a unit for generating additional information (n).

31. The apparatus of claim 30, wherein unit for generating additional information (n) is a random number generator and where the additional information (n) is a random number, preferably an unpredictable random number.

32. The apparatus of claim 26 being part of a computer system.

33. The apparatus of claim 26 being part of a mobile computer system or part of a vehicle, such as a rental car.

34. Apparatus comprising:

- a network interface (67) for connecting the apparatus (13; 23; 61) via a network (12; 22; 62, 66, 68) to a computer system (11; 21; 60);
- a processor (71);
- a memory (72) with code which, when being executed by the processor (71), performs the steps:
  - receiving an identifier (w) from the computer system (11; 21; 60) via the network (12; 22; 62, 66, 68) and the network interface (67);
  - comparing the identifier (w) with a list (14; 24) of identifiers (w) to determine whether the identifier (w) originates from a computer system (11; 21; 60) that was reported lost or stolen; and
    - if the identifier (w) originates from a computer system (11; 21; 60) that was not reported lost or stolen, then generating a token (S) which comprises the identifier (w) and a credit (C), signing the token (S) using a cryptographic key to create a signed token (S), and sending the signed token (S) via the network interface (67) and the network (12; 22; 62, 66, 68) to the computer system (11; 21; 60).

35. The apparatus of claim 34, whereby the credit (C) is a revocation credit.

36. The apparatus of claim 34, whereby the apparatus is part of a server or server module.

37. The apparatus of claim 34, whereby the cryptographic key is a public key.

38. The apparatus of claim 34, whereby the list (14; 24) of identifiers (w) is a black-list which comprises the identifier (w) of a plurality of computer systems that are reported lost or stolen.

39. The apparatus of claim 34, whereby the list (14; 24) of identifiers (w) is a valid list which comprises the identifier (w) of a plurality of computer systems that are not reported lost or stolen.

40. A computer program product comprising a computer readable medium, having thereon:

computer program code means, when said program is loaded in a computer system (11; 21; 60), which comprises a communication interface (64) for connection via a network (12; 22; 62) to a server module (13; 23; 61), execute procedure to

a. exhaust step-by-step a credit of a credit counter (44) of the computer system (11; 21; 60) ;

b. switch the computer system (11; 21; 60) into the special mode of operation if the credit is exhausted;

c. send an identifier (w) assigned to the computer system (11; 21; 60) via the communication interface (64) and the network (12; 22; 62) to the server module (13; 23; 61);

d. receive a token (S) issued by the server module (13; 23; 61);

e. verify the validity of the token (S); and

f. if the token (S) is valid, then extract a credit (C) from the token (S) and updating the credit counter (44) with the credit (C).

41. The computer program product of claim 40, whereby the computer system (11; 21; 60) is caused to switch into the special mode of operation if step e. reveals that the token (S) is invalid.

42. The computer program product of claim 40, whereby the computer system (11; 21; 60) continues with step c. if step e. reveals that the token (S) is invalid.

43. A computer program element comprising:

computer program code means to make a computer system (11; 21; 60), which comprises a communication interface (64) for connection via a network (12; 22; 62) to a server module (13; 23; 61), execute procedure to

a. exhaust step-by-step a credit of a credit counter (44) of the computer system (11; 21; 60) ;

b. switch the computer system (11; 21; 60) into the special mode of operation if the credit is exhausted;

c. send an identifier (w) assigned to the computer system (11; 21; 60) via the communication interface (64) and the network (12; 22; 62) to the server module (13; 23; 61);

d. receive a token (S) issued by the server module (13; 23; 61);

e. verify the validity of the token (S); and

f. if the token (S) is valid, then extract a credit (C) from the token (S) and updating the credit counter (44) with the credit (C).

44. A computer program product comprising a computer readable medium, having thereon:

computer program code means, when said program is loaded in a server (11; 21; 60), which comprises a network interface (67) for connection via a network (12; 22; 62, 66, 68) to a computer system (11; 21; 60), execute procedure to

- receive an identifier (w) from the computer system (11; 21; 60) via the network (12; 22; 62, 66, 68) and the network interface (67);

- compare the identifier (w) with a list (14; 24) of identifiers (w) to determine whether the identifier (w) originates from a computer system (11; 21; 60) that was reported lost or stolen;

  - if the identifier (w) originates from a computer system (11; 21; 60) that was not reported lost or stolen, then generating a token (S) which comprises the identifier (w) and a credit C, signing the token (S) using a cryptographic key to create a signed token (S), and sending the signed token (S) via the network interface (67) and the network (12; 22; 62, 66, 68) to the computer system (11; 21; 60).

45. A computer program element comprising:

computer program code means to make a server (11; 21; 60), which comprises a network interface (67) for connection via a network (12; 22; 62, 66, 68) to a computer system (11; 21; 60), execute procedure to

- receive an identifier (w) from the computer system (11; 21; 60) via the network (12; 22; 62, 66, 68) and the network interface (67);

- compare the identifier (w) with a list (14; 24) of identifiers (w) to determine whether the identifier (w) originates from a computer system (11; 21; 60) that was reported lost or stolen;

- if the identifier (w) originates from a computer system (11; 21; 60) that was not reported lost or stolen, then generating a token (S) which comprises the identifier (w) and a credit C, signing the token (S) using a cryptographic key to create a signed token (S), and sending the signed token (S) via the network interface (67) and the network (12; 22; 62, 66, 68) to the computer system (11; 21; 60).